Dragon® 7 Network Intrusion Detection and Prevention

- Stealth Network Intrusion Prevention appliances that stop offenders from ever entering the network
- New industry-leading VoIP protocol decoders protect network from DOS attacks
- High-speed Gigabit capacity for network defense
- Zero Day event detection using a comprehensive multi-method approach
- Key component of Enterasys' Dynamic Intrusion Response solution

Data Sheet

- **In-line Network Intrusion Prevention appliances**
  - Protects the network from attackers and keeps them from returning
- **High performance architecture**
  - Gigabit-speed performance even with protocol decoding, anomaly detection and pattern matchers, active simultaneously
- **Virtual Sensor support**
  - Allows one sensor to act as multiple unique sensors
- **Protocol decoding**
  - New VoIP decoders identify attackers who hide an attack within the protocol
- **New state-of-the-art signature language**
  - Incorporates regular expressions, compound pattern matchers, thresholding and state tracking
- **IDS/IPS Evasion Counter Measures**
  - Identifies/blocks attackers who attempt to evade Dragon with fragmented packets and streams
- **Dynamic response**
  - Enables Enterasys' DIR; supports provisioning response actions in firewalls, switches, routers
- **Event sniping**
  - Terminates an attack session via a TCP reset or ICMP unreachable message
- **Probe prevention**
  - Defeats scanning techniques with false responses

Powerful Network Intrusion Defense

A sophisticated software- and appliance-based network intrusion defense system, the Dragon Network Sensor identifies misuse and attacks across the network.

Dragon's advanced **Intrusion Prevention** (IPS) technology is designed to block attackers, mitigate denial of service attacks and prevent information theft while remaining totally invisible to the network. Built upon Dragon's award-winning Intrusion Detection technology, the IPS will alert on the attack, drop the offending packets, terminate the session for TCP- and UDP-based attacks, and dynamically establish firewall rules that can keep the source of the threat off the network indefinitely or for a configurable period of time. Known sources of attacks can be stopped from ever entering the network by enabling "**Black Lists**," while key corporate resources or trusted networks are always allowed to pass via "**White Lists**."

Dragon comes ready "out of the box" with a large library of attacks it can be configured to mitigate immediately. Dragon's Network IPS can leverage the thousands of vulnerability- and exploit-based signatures in Dragon's threat libraries as a basis for network control and threat defense.

Dragon IPS is available only on currently shipping Dragon appliances. However, it's important to note that almost all of the Dragon IDS appliances can be converted into IPS appliances by simply purchasing an add-on license. Customers are not required to buy all new appliances if they want to specify certain ones for IPS. Dragon's IPS appliances ensure a high degree of reliability and redundancy, including fail-safe bypass options.

Placed at the network edge or at key aggregation points, the Dragon Network Sensor is unmatched in detecting security events such as network misuse, network intrusions, system exploits and virus or spyware propagations. Dragon uses a multimethod approach to identify attacks: pattern matching, protocol analysis and anomaly-based techniques. Application-based event detection detects non-signature-based attacks against commonly targeted applications including HTTP, RPC and FTP.

With Dragon 7.2, industry-leading VOIP protocol decoders are provided for SIP and H.323, which can identify malformed messages and prevent damaging DOS attacks. Also with Dragon 7.2, a new state-of-the-art signature language is introduced, which provides the ability to test arithmetical byte sequences, combined with multiple pattern matches and Perl Compatible Regular Expressions while maintaining state. Thresholding can now be done at the signature level and is customizable for each virtual sensor. Signatures continue to be in an open tunable XML based format.

enterasys™
Networks that Know

Additionally, many Dragon signatures and alert options are designed to detect Zero Day attacks. These multimethod detection techniques— combined with an extensive, frequently updated signature database and false positive tuning capabilities— ensure that no threat and policy violations go undetected.

Dragon's **Adaptive Match Engine** and multithreaded application gain significant performance through software. The profile of network traffic flowing through the sensor is analyzed and then one of nine algorithms is "adaptively" selected to analyze the traffic. In this way, the Sensor can use multiple detection algorithms simultaneously while intelligently applying each to the type of traffic it is best suited to analyze.

Dragon **Virtual Sensors** allow for flexible deployments in diverse environments by enabling security administrators to configure a single sensor to operate as if it is multiple unique sensors. Dragon's Virtual Sensors apply to both IDS and IPS sensors, and can be associated with Virtual LANs, IP networks, physical ports, or even TCP and UDP level applications. Each sensor can be configured with unique policies that define what analysis techniques will be utilized and what event alerts will be generated. Through Dragon's Virtual Sensor technology, a single Dragon system can act as an IDS and an IPS at the same time.

In addition to Intrusion Prevention actions, the Network Sensor can employ a variety of **Active Response** techniques to block would-be intruders, worms or network misusers by taking action either to terminate the threat session directly or by reconfiguring firewalls, or switch and router policies to block ongoing attempts to attack. Dragon Network Sensors are also an integral part of Enterasys' Dynamic Intrusion Response (DIR) solution, which provides pinpoint threat mitigation down to its point of entry into the campus. DIR works in wired and wireless networks and can quarantine, filter or disable network access for the sources of the Dragon-detected threat.

Dragon Network Sensor offers market-leading deep forensics capabilities, including flexible packet capture and complete session reconstruction. which are essential to analyzing network-based attacks. It also offers **pre-event collection**, capturing packets preceeding, but related to, packets that triggered an attack.

Dragon Network Sensor is centrally managed via Dragon **Enterprise Management Server**, which provides easy signature and configuration management with live updates. Customers can easily monitor the activities of their IDS and IPS since all actions taken and threats detected are reported into Dragon's management reporting system.

Specifications

Technical Specifications

IDS Software

Dragon Network Sensor Software for Ethernet
Part Numbers: DSNSS7-E
Performance rating: 20 Mbps

Dragon Network Sensor Software for Fast Ethernet
Part Numbers: DSNSS7-FE
Performance rating: 200 Mbps

Dragon Network Sensor Software for Gigabit Ethernet
Part Numbers: DSNSS7-GE
Performance rating: 1 Gbps or greater

Network Sensor Software is supported on the following operating systems:
Fedora Core, Redhat Enterprise, Sun Solaris

Technical Specifications

IDS/IPS Appliances

FE100 Dragon Network Sensor Appliance
Part Numbers: DSNSA7-FE100-TX
Performance rating: 100 Mbps
Architecture: Intel Celeron
Memory: 1 GB, 40 GB IDE hard drive
NICs: 2 10/100 copper, 1 10/100/1000 copper
Plus, 1 10/100/1000 copper for IPS appliance
(2 ports on the IPS are fail-safe bypass)

GE250 Dragon Network Sensor Appliance
Part Numbers: DSNSA7-GE250-TX/SX
Performance rating: 250 Mbps
Architecture: Intel Pentium 4
Memory: 1 GB, minimum 36 GB hard drive
NICs: 2 10/100/1000 copper, plus 1 Gigabit fiber or 1 Gigabit copper NIC configuration
Plus, 1 10/100/1000 copper for IPS appliance
(2 ports on the IPS are fail-safe bypass)

GE500 Dragon Network Sensor Appliance
Part Numbers: DSNSA7-GE500-TX/SX
Performance rating: 500 Mbps
Architecture: Dual Intel XEON
Memory: 1 GB, minimum 36 GB hard drive
NICs: 2 10/100/1000 copper, plus 2 Gigabit fiber or 2 Gigabit copper NIC configuration
(2 ports on the IPS are fail-safe bypass)

GIG Dragon Network Sensor Appliance
Part Numbers: DSNSA7-GIG-TX/SX
Performance rating: 1+ Gbps
Architecture: Dual Intel XEON
Memory: 2 GB, minimum 36 GB hard drive
NICs: 2 10/100/1000 copper, plus 4 Gigabit fiber or 4 Gigabit copper NIC configuration
Redundant power and cooling standard
(4 ports on the IPS are fail-safe bypass)

Physical Specifications

Form Factor
1U rack-mount server chassis for EIA standard 310-D racks

Dimensions
4.32 cm (1.7") H X 42.9 cm (16.9") W X 58.42 cm (23") D (FE100 only)
4.32 cm (1.7") H X 42.9 cm (16.9") W X 60.71cm (23.9") D

2U rack-mount server chassis for EIA standard 310-D racks

Dimensions
8.8 cm (3.4") H X 42.9 cm (16.9") W X 60.71cm (23.9") D

Front Panel (Buttons)
Power on/off button, system-reset button, ACPI sleep switch system ID button, and tool-activated NMI switch (FE100 only)

Front Panel (LEDs)
Power, hard drive activity, network activity (two), and general system fault

Environmental Specifications

Operating Temperature
+5° C to +35° C (41° F to 95° F)
(maximum change not to exceed +10° C)

Non-Operating Temperature
-40° C to +70° C (-40° F to 158° F) (ambient)

Non-Operating Humidity
95% at 35° C (non-condensing)

Power Consumption
Voltage Range: 4.96 Amp at 115V
Voltage Range: 2.48 Amp at 220V

Specifications (continued)

Agency and Standards Specifications

Safety

Argentina: IRAM Certificate
Australia/New Zealand: ACA/MED (FE100 only)
Belarus: Bellis Certificate (FE100 only)
Canada: UL 60950 – CSA 60950 (UL and cUL)
China: CNCA (FE100 only), GB4943 (CCC certification)
Europe/CE Mark: EN60950 (complies with 73/23/EEC)
Germany: GS License
International: IEC60950 (CB Report and Certificate)
Nordic Countries: EMKO – TSE (74-SEC) 207/94 (excluding FE100)
Russia: GOST 50377-92
U.S.: UL60950 – CSA 60950 (UL and cUL)
U.S.: FCC, Part 15

Electromagnetic Compatibility (EMC) (Class A)

Australia/New Zealand: AS/NZS 3548 (based on CISPR 22)
Canada: ICES-003
China:GB 9254 and GB 17625 (CCC certification)
Europe/CE Mark: EN55022, EN55024 and EN61000-3-2;-3-3 (complies with 89/336/EEC)
International: CISPR 22
Japan: VCCI
Korea: RRL, MIC 1997-41 and 1997-42

Russia: GOST 29216-91 and 50628-95
Taiwan: CNS13438 (excluding FE100), BSMI RPC (FE 100 only)
U.S.: FCC, Part 15

Ordering Information

Network IDS Software

DSNSS7-E
20 Mbps performance license

DSNSS7-FE
200 Mbps performance license

DSNSS7-GE
1000 Mbps performance license

Network IPS Appliances

DSIPA7-FE100-TX
Dragon FE100 Network IPS Appliance for the small/branch office (copper fail-safe bypass network interface card)

DSIPA7-GE250-TX
Dragon GE250 Network IPS Appliance for the regional office, small data center (copper fail-safe bypass gigabit network interface card)

DSIPA7-GE250-SX
Dragon GE250 Network IPS Appliance for the regional office, small data center (fiber fail-safe bypass gigabit network interface card)

DSIPA7-GE500-TX
Dragon GE500 Network IPS Appliance for the data center (copper fail-safe bypass gigabit network interface card)

DSIPA7-GE500-SX
Dragon GE500 Network IPS Appliance for the data center (fiber fail-safe bypass gigabit network interface card)

DSIPA7-GIG-TX
Dragon GIG Network IPS Appliance for the data center (copper fail-safe bypass gigabit network interface card)

DSIPA7-GIG-SX
Dragon GIG Network IPS Appliance for the data center (fiber fail-safe bypass gigabit network interface card)

Ordering Information (continued)

Network IPS Add-Ons to Existing Dragon IDS Appliances

DSIPS7-FE100-TX
Dragon IPS Add-on to FE100, includes copper fail-safe bypass dual-port network interface card

DSIPS7-GE250-TX
Dragon IPS Add-on to GE250, includes copper fail-safe bypass dual-port network interface card

DSIPS7-GE250-SX
Dragon IPS Add-on to GE250, includes fiber fail-safe bypass dual-port network interface card

DSIPS7-GE500-TX
Dragon IPS Add-on to GE500, includes copper fail-safe bypass dual-port network interface card

DSIPS7-GE500-SX
Dragon IPS Add-on to GE500, includes fiber fail-safe bypass dual-port network interface card

DSIPS7-GIG-TX
Dragon IPS Add-on to GIG, includes 2 copper fail-safe bypass dual-port network interface cards

DSIPS7-GIG-SX
Dragon IPS Add-on to GIG, includes 2 fiber fail-safe bypass dual-port network interface cards

Network IDS Appliances

DSNSA7-FE100-TX
Dragon FE100 Network Sensor Appliance for the small/branch office (copper interface card)

DSNSA7-GE250-TX
Dragon GE250 Network Sensor Appliance for the regional office, small data center (copper gigabit network interface card)

DSNSA7-GE250-SX
Dragon GE250 Network Sensor Appliance for the regional office, small data center (fiber gigabit network interface card)

DSNSA7-GE500-TX
Dragon GE500 Network Sensor Appliance for the data center (copper gigabit network interface card)

DSNSA7-GE500-SX
Dragon GE500 Network Sensor Appliance for the data center (fiber gigabit network interface card)

DSNSA7-GIG-TX
Dragon GIG Network Sensor Appliance for the data center (copper gigabit network interface card)

DSNSA7-GIG-SX
Dragon GIG Network Sensor Appliance for the data center (fiber gigabit network interface card)

Warranty

As a customer-centric company, Enterasys is committed to providing the best possible workmanship and design in our product set. The Dragon product family includes a ninety (90) day warranty for software that covers defects in media only, and a one (1) year warranty for hardware.

Service and Support

Enterasys understands that superior service and support is a critical component of ***Networks that Know***.™ The Enterasys **SupportNet Portfolio**—a suite of innovative and flexible service and support offerings—completes the Enterasys solution. SupportNet offers all the post-implementation support services you need—online, onsite or over the phone—to maintain your network availability and performance.

Additional Information

For more information about Enterasys Dragon, visit the web at **http://www.enterasys.com/products/ids**

Contact Information

Contact Enterasys Sales at **877-801-7082** or **enterasys.com/corporate/contact/contact-sales.html**

Enterasys Networks
Corporate Headquarters
50 Minuteman Road
Andover, MA 01810
U.S.A

Dragon is a registered trademark of Enterasys Networks. All other products or services mentioned are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

All contents are copyright © 2006 Enterasys Networks, Inc. All rights reserved.

Lit. #9013766-4 1/06

enterasys™
Networks that Know